IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 10/782,678
Filing Date ..... February 19, 2004
Inventorship ..... Zigmond
Applicant ..... Microsoft Corp.
Group Art Unit 3621
Examiner ..... Agwumezie, Charles C.
Old Docket No. MS1-1838US
Attorney's Docket No. MS-306815.01
Title: Persistent License for Stored Content

To: The Honorable Commissioner for Patents
Mail Stop Appeal Brief- Patents
PO Box 1450
Alexandria, Virginia 22313-1450

From: William J. Breen III (Tel. 509.755.7253; Fax 509.755.7252)
Customer No. 22971

BRIEF OF APPELLANT

The Applicant has filed a timely Notice of Appeal from the action of the Examiner in finally rejecting all of the claims that were considered in this application. This Brief is being filed under the provisions of 37 C.F.R. § 1.192. The Filing Fee, as set forth in 37 C.F.R. § 1.17(c), is submitted herewith.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is Microsoft Corporation, by way of assignment from Zigmond et al., who is the named inventive entity and is captioned in the present brief.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1-42 are pending and are the subject of this appeal.

STATUS OF AMENDMENTS

None.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Protection of stored content may be maintained through use of a persistent license. The persistent license may include one or more keys that are encrypted such that the client may not access the keys. The persistent license, however, may be decrypted (e.g., by a licensing server) to obtain the included keys. Therefore, when the client desires access to stored content, the client communicates the persistent license to the licensing server. The licensing server may then verify access rights of the client. If the client has rights to the content, the licensing server communicates a license that includes the key from the persistent license such that the client may access the content. In an implementation, the client may utilize the key to decrypt the content directly, i.e. the key is utilized to decrypt the content. In another implementation, the client may utilize the key to decrypt a content license to obtain a content key, which is then utilized to decrypt the content. In a further implementation, additional key hierarchies are employed to provide additional encryption. *See Application, Paragraph [0022] and FIGS. 1, 7 and 8.*

Independent Claim 1 recites a method comprising:

- forming a request (e.g., reference number 722, FIG. 7; paragraphs [0065]-[0067], pages 27-28) by a client (e.g., reference number 104, FIG. 7; paragraphs [0065]-[0067], pages 27-28) to access encrypted content, wherein:

- the request includes a persistent license (e.g., reference number 708, FIG. 7; paragraphs [0065]-[0067], pages 27-28) for communication to a licensing server (e.g., reference number 126, FIG. 7; paragraphs [0065]-[0067], pages 27-28); and
- the persistent license includes a key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28) that is encrypted such that the key is not accessible by the client (e.g., reference number 104, FIG. 7; paragraphs [0065]-[0067], pages 27-28); and

- receiving a license (e.g., reference number 726, FIG. 7; paragraphs [0065]-[0067], pages 27-28) in response to the request, wherein the received license includes the key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28) that is:
  - accessible by the client (e.g., reference number 104, FIG. 7; paragraphs [0065]-[0067] , FIG. 7; pages 27-28); and
  - for accessing the encrypted content paragraphs (e.g., reference number 716, FIG. 7; [0065]-[0067], pages 27-28.

Independent Claim 11 recites a method comprising:

- forming a request (e.g., reference number 702, FIG. 7; paragraphs [0062]-[0067], pages 26-28) by a client (e.g., reference number 104, FIG. 7; paragraphs [0062]-

[0067], pages 26-28) for communication to a licensing server (e.g., reference number 126, FIG. 7; paragraphs [0065]-[0067], pages 27-28), wherein the request is for storing encrypted content by the client (e.g., reference number 104, FIG. 7; paragraphs [0062]-[0067], pages 26-28);

- receiving a persistent license request at the client (e.g., reference number 104, FIG. 7; paragraphs [0062]-[0067], pages 26-28) in response to the request, wherein:
    - the persistent license (e.g., reference number 706, FIG. 7; paragraphs [0062]-[0067], pages 26-28) includes a key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28) that is encrypted;
    - the key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28), when decrypted, provides access to the encrypted content;
    - the key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28) is configured to be decrypted by the licensing server (e.g., reference number 126, FIG. 7; paragraphs [0065]-[0067], pages 27-28); and
    - the client (e.g., reference number 104, FIG. 7; paragraphs [0062]-[0067], pages 26-28) is not configured to decrypt the key (e.g.,

reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28) from the persistent license; and

- storing the persistent license and the encrypted content by the client (e.g., reference number 104, FIG. 7; paragraphs [0062]-[0067], pages 26-28).

Independent Claim 17 recites a method comprising:

- forming a first request (e.g., reference number 702, FIG. 7; paragraphs [0062]-[0067], pages 26-28) for communication to a licensing server (e.g., reference number 126, FIG. 7; paragraphs [0065]-[0067], pages 27-28), wherein the first request is for storing encrypted content;
- receiving a persistent license (e.g., reference number 708, FIG. 7; paragraphs [0065]-[0067], pages 27-28) in response to the request, wherein the persistent license (e.g., reference number 708, FIG. 7; paragraphs [0065]-[0067], pages 27-28) includes a boundary key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28);
- storing the persistent license (e.g., reference number 708, FIG. 7; paragraphs [0065]-[0067], pages 27-28) and the content;
- forming a second request (e.g., reference number 722, FIG. 7; paragraphs [0065]-[0067], pages 27-28) to access the encrypted content, wherein the second request includes the persistent license (e.g., reference number 708, FIG. 7; paragraphs

[0065]-[0067], pages 27-28);

- sending the second request to the licensing server (e.g., reference number 126, , FIG. 7; paragraphs [0065]-[0067], pages 27-28);
- receiving a boundary license (e.g., reference number 726, FIG. 7; paragraphs [0065]-[0067], pages 27-28) in response to the second request, wherein the boundary license includes the boundary key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28);
- decrypting the boundary license (e.g., reference number 726, FIG. 7; paragraphs [0065]-[0067], pages 27-28) using a session key to obtain the boundary key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28);
- decrypting a content license (e.g., reference number 712, FIG. 7; paragraphs [0065]-[0067], pages 27-28) using the boundary key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28) to obtain a content key (e.g., reference number 714; FIG. 8; paragraph [0076], page 30); and
- decrypting the encrypted content (e.g., reference number 716; FIG. 8; paragraph [0076], page 30) using the content key (e.g., reference number 714; FIG. 8; paragraph [0076], page 30).

Independent Claim 23 recites a client comprising:

- a processor (e.g., reference number 204, FIG. 2; paragraph [0030],.Page 12); and

- memory (e.g., reference number 206, FIG. 2; paragraph [0030],. Page 12);configured to maintain:
    - a persistent license (e.g., reference number 708, FIG. 7; paragraphs [0065]-[0067], pages 27-28) including a key that is encrypted; and
    - a playback application (e.g., reference number 136, FIG. 2; paragraph [0028], Page 12);that is executable on the processor to:
        - form a request (e.g., reference number 722, FIG. 7; paragraphs [0065]-[0067], pages 27-28) to access encrypted content, wherein the request:
            - is for communication to a licensing server (e.g., reference number 126, FIG. 7; paragraphs [0065]-[0067], pages 27-28); and
            - includes the persistent license (e.g., reference number 708, FIG. 7; paragraphs [0065]-[0067], pages 27-28);
        - receive a response to the request (e.g., reference number 726, FIG. 7; paragraphs [0065]-[0067], pages 27-28) that includes the key(e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28); and
        - access the encrypted content utilizing the key(e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-

28).

Independent Claim 33 recites a client comprising:

- a network (e.g., reference number 106, FIG. 1; paragraph [0023], pages 8-9);
- a client (e.g., reference number 104, FIG. 7; paragraphs [0065]-[0067], pages 27-28)including:
    - a persistent license (e.g., reference number 708, FIG. 7; paragraphs [0065]-[0067], pages 27-28) having a key that is encrypted; and
    - a playback application that is executable to:
        - form a request to access encrypted content, wherein the request includes the persistent license (e.g., reference number 708, FIG. 7; paragraphs [0065]-[0067], pages 27-28);
        - receive a response to the request that includes the key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28); and
        - access the encrypted content utilizing the key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28); and
- a licensing server (e.g., reference number 126, FIG. 7; paragraphs [0065]-[0067],

pages 27-28) including a licensing module (e.g., reference number 128, FIG. 7; paragraphs [0065]-[0067], pages 27-28) that is executable to:

- receive the request including the persistent license (e.g., reference number 708, FIG. 7; paragraphs [0065]-[0067], pages 27-28);
- decrypt the persistent license (e.g., reference number 708, FIG. 7; paragraphs [0065]-[0067], pages 27-28) to obtain the key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28); and
- form the response (e.g., reference number 726, FIG. 7; paragraphs [0065]-[0067], pages 27-28) that includes the key (e.g., reference number 710, FIG. 7; paragraphs [0065]-[0067], pages 27-28) for communication to the client (e.g., reference number 104, FIG. 7; paragraphs [0065]-[0067], pages 27-28) over the network.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-42 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Printed Patent Application No. 2003/0028488 to Mohammed et al. (hereinafter "Mohammed").

ARGUMENT

First Ground of Rejection Claims 1-42 satisfy the requirements of 35 U.S.C. § 102(b) and therefore are not unpatentable over Mohammed.

Claim 1 recites a method comprising:

- forming a request by a client to access encrypted content, wherein:
  - the request includes a persistent license for communication to a licensing server; and
  - the persistent license includes a key that is encrypted such that the key is not accessible by the client; and
- receiving a license in response to the request, wherein the received license includes the key that is:
  - accessible by the client; and
  - for accessing the encrypted content.

It is respectfully submitted that Mohammed does not disclose these features.

Beginning at page 8 of the subject application, an exemplary use of a persistent license is described. The persistent license of the client includes a key that may be used to access encrypted content, but the key is encrypted such that the client may not access the key. The persistent license, however, may be decrypted by a licensing server to obtain the included key. Therefore, when the client desires access to stored content, the client communicates the persistent license to the licensing server.

The licensing server may then verify access rights of the client. If the client has rights to the content, the licensing server communicates a license that includes the key from the persistent license such that the client may access the content. In an

implementation, the client may utilize the key to decrypt the content directly, i.e. the key is utilized to decrypt the content. In another implementation, the client may utilize the key to decrypt a content license to obtain a content key, which is then utilized to decrypt the content. In either case, the key used to access the content is included in the persistent license and communicated to the licensing service.

Mohammed, on the other hand, does not show the communication of an encrypted key **from the client**, which is then decrypted by the licensing server and **communicated back to the client** to access the content. The Office in rejecting Claim 1 asserts the following portion of Mohammed:

> [0016] Importantly, the license server only issues a license to a DRM system that is `trusted` (i.e., that can authenticate itself). To implement `trust`, the DRM system is equipped with a `black box` that performs decryption and encryption functions for such DRM system. The black box includes a public/private key pair, a version number and a unique signature, all as provided by an approved certifying authority. The public key is made available to the license server for purposes of encrypting portions of the issued license, thereby binding such license to such black box. The private key is available to the black box only, and not to the user or anyone else, for purposes of decrypting information encrypted with the corresponding public key. The DRM system is initially provided with a black box with a public/private key pair, and the user is prompted to download from a black box server an updated secure black box when the user first requests a license. The black box server provides the updated black box, along with a unique public/private key pair. Such updated black box is written in unique executable code that will run only on the user's computing device, and is re-updated on a regular basis.
>
> [0017] When a user requests a license, the client machine sends

> the black box public key, version number, and signature to the license server, and such license server issues a license only if the version number is current and the signature is valid. A license request also includes an identification of the digital content for which a license is requested and a key ID that identifies the decryption key associated with the requested digital content. The license server uses the black box public key to encrypt the decryption key, and the decryption key to encrypt the license terms, then downloads the encrypted decryption key and encrypted license terms to the user's computing device along with a license signature. *See Mohammed, Paragraphs [0016]-[0017].*

Thus, as shown in the above excerpt, the client machine sends the black box public key, version number and signature. However, none of these sent items is disclosed as "a key that is encrypted such that the key is not accessible by the client" that once received in a license is usable "for accessing the encrypted content" as recited in Claim 1. Rather, the public key communicated by the client machine of Mohammed is accessible by the client and is communicated to the license server to encrypt the decryption key. Therefore, the public key of Mohammed is also not communicated back to the client, as the client already has the public key that is accessible by the client. Further, Mohammed does not disclose that the public key is not accessible by the client machine as recited in Claim 1. Therefore, it is respectfully submitted that Claim 1 is allowable.

Claims 2-10 depend either directly or indirectly from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in

claim 1, are neither shown nor suggested in the references of record, either singly or in combination with one another.

Claim 11 is allowable based on similar reasoning previously mentioned with respect to claim 1, as well as for its own recited features. In particular, Claim 11 recites receipt of a persistent license at the client, in which, "**the persistent license includes a key that is encrypted**", "**the key, when decrypted, provides access to the encrypted content**", "**the key is configured to be decrypted by the licensing server**", and "**the client is not configured to decrypt the key from the persistent license**". Therefore, as previously described the client includes the key that is communicated to the licensing server for decryption. It is respectfully submitted that Claim 11 is allowable over the references of record.

Claims 12-16 depend either directly or indirectly from claim 11 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 11, are neither shown nor suggested in the references of record, either singly or in combination with one another.

Claim 17 is allowable based on similar reasoning previously mentioned with respect to claim 1, as well as for its own recited features. In particular, Claim 17 recites "receiving a persistent license in response to the request, **wherein the persistent license includes a boundary key**", "forming a second request to access

the encrypted content, **wherein the second request includes the persistent license**", "sending the second request to the licensing server" and "**receiving a boundary license in response to the second request, wherein the boundary license includes the boundary key**". Therefore, as previously described the key is originally available by an entity (e.g., a client) that performs these steps and is provided by that entity to a licensing server for decryption. It is respectfully submitted that Claim 17 is allowable and withdrawal of the rejection is respectfully requested.

Claims 18-22 depend either directly or indirectly from claim 17 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 17, are neither shown nor suggested in the references of record, either singly or in combination with one another.

Claim 23 is allowable based on similar reasoning previously mentioned with respect to claim 1, as well as for its own recited features. In particular, Claim 23 recites a client having "**a persistent license including a key** that is encrypted" and "a playback application that is executable on the processor to: **form a request** to access encrypted content, wherein the request: is for communication to a licensing server; and **includes the persistent license**; **receive a response to the request that includes the key**; and **access the encrypted content utilizing the key**." Therefore, it is respectfully submitted that Claim 23 is allowable.

Claims 24-32 depend either directly or indirectly from claim 23 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 23, are neither shown nor suggested in the references of record, either singly or in combination with one another.

Claim 33 is allowable based on similar reasoning previously mentioned with respect to claim 1, as well as for its own recited features. In particular, Claim 33 recites "**a persistent license having a key** that is encrypted" and "a playback application that is executable to: **form a request** to access encrypted content, wherein **the request includes the persistent license**; **receive a response to the request that includes the key**; and **access the encrypted content utilizing the key**". Therefore, it is respectfully submitted that Claim 33 is allowable and withdrawal of the rejection is respectfully requested.

Claims 34-42 depend either directly or indirectly from claim 33 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 33, are neither shown nor suggested in the references of record, either singly or in combination with one another.

Accordingly, it is respectfully submitted that a *prima facie* case of obviousness has not been established. Therefore, the Applicant respectfully requests that the Board overturn the First Ground of Rejection.

CONCLUSION

The Applicant respectfully considers this application to be in condition for allowance and respectfully requests the Board to overturn the final rejection and that the Examiner pass this application to allowance.

Dated this 26th day of February, 2007.

Respectfully submitted,

/William J. Breen, III #45,313/
WILLIAM J. BREEN, III
Attorney for Applicant
Registration No. 45,313

Sadler, Breen, Morasch and Colby, p.s.
422 W. Riverside Ave., Suite 424
Spokane, WA 99201
509.755.7253

APPENDIX: CLAIMS ON APPEAL

1. (original): A method comprising:

forming a request by a client to access encrypted content, wherein:

the request includes a persistent license for communication to a licensing server; and

the persistent license includes a key that is encrypted such that the key is not accessible by the client; and

receiving a license in response to the request, wherein the received license includes the key that is:

accessible by the client; and

for accessing the encrypted content.

2. (original): A method as described in claim 1, further comprising:

forming an initial request for:

communication to the licensing server; and

storing encrypted content by the client;

receiving the persistent license at the client in response to the initial request; and

storing the encrypted content and the persistent license by the client.

3. (original): A method as described in claim 1, further comprising:

forming an initial request by another client for:

communication to the licensing server; and

storing encrypted content by the other client;

receiving the persistent license at the other client in response to the initial request;

storing the encrypted content and the persistent license by the other client; and

obtaining the persistent license by the client from the other client.

4. (original): A method as described in claim 1, wherein the received license is a boundary license and the key is a boundary key, and further comprising:

decrypting a session license utilizing a client key to obtain a session key;

decrypting the boundary license utilizing the session key to obtain the boundary key;

decrypting a content license utilizing the boundary key to obtain a content key; and

decrypting the encrypted content utilizing the content key.

5. (original): A method as described in claim 4, wherein:

the session license includes access rules for the client for a session initiated between the client and the licensing server;

the boundary license includes access rules for the client for the encrypted content that is within a rights boundary in the encrypted content; and

the content license includes access rules for the client for the encrypted content.

6. (original): A method as described in claim 4, wherein:

the persistent license was encrypted using an asymmetric encryption algorithm; and

the encrypted content, the boundary license, and the content license were encrypted using respective symmetric encryption algorithms.

7. (original): A method as described in claim 1, further comprising:

decrypting a session license utilizing a client key to obtain a session key, wherein the session license includes access rules for a session initiated between the client and the licensing server;

decrypting the received license utilizing the session key to obtain a decrypted boundary license, wherein:

the received license is an encrypted boundary license and the key within the boundary license is a boundary key; and

the boundary license includes access rules for content within a rights boundary in the encrypted content that is at least one of a television program and a television channel;

decrypting a content license utilizing the boundary key to obtain a content key, wherein the content license includes access rules for the encrypted content; and

decrypting the encrypted content utilizing the content key, wherein the encrypted content includes at least a portion of a television broadcast.

8. (original): A method as described in claim 1, wherein the key is for decrypting the encrypted content.

9. (original): A method as described in claim 1, wherein the encrypted content is streamed to the client.

10. (original): One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 1.

11. (original): A method comprising:

forming a request by a client for communication to a licensing server, wherein the request is for storing encrypted content by the client;

receiving a persistent license at the client in response to the request, wherein:

the persistent license includes a key that is encrypted;

the key, when decrypted, provides access to the encrypted content;

the key is configured to be decrypted by the licensing server; and

the client is not configured to decrypt the key from the persistent license; and

storing the persistent license and the encrypted content by the client.

12. (original): A method as described in claim 11, further comprising:

forming a subsequent request by the client to access the stored content, wherein the subsequent request:

is for communication to the licensing server; and

includes the persistent license; and

receiving a second license at the client in response to the subsequent request, wherein:

the second license includes the key; and

the second license is configured to be decrypted by the client such that the client obtains access to the key.

13. (original): A method as described in claim 11, further comprising:

forming a subsequent request by another client to access the stored content, wherein the subsequent request:

is for communication to the licensing server; and

includes the persistent license; and

receiving a second license at the other client in response to the subsequent request, wherein:

the second license includes the key; and

the second license is configured to be decrypted by the other client such that the other client obtains access to the key.

14. (original): A method as described in claim 11, wherein the encrypted content is streamed to the client.

15. (original): A method as described in claim 11, wherein the license includes a certificate for verifying the licensing server by the client.

16. (original): One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 11.

17. (original): A method comprising:

forming a first request for communication to a licensing server, wherein the first request is for storing encrypted content;

receiving a persistent license in response to the request, wherein the persistent license includes a boundary key;

storing the persistent license and the content;

forming a second request to access the encrypted content, wherein the second request includes the persistent license;

sending the second request to the licensing server;

receiving a boundary license in response to the second request, wherein the boundary license includes the boundary key;

decrypting the boundary license using a session key to obtain the boundary key;

decrypting a content license using the boundary key to obtain a content key; and

decrypting the encrypted content using the content key.

18. (original): A method as described in claim 17, wherein the forming of:

the first request is performed by a first client; and

the second request is performed by a second client.

19. (original): A method as described in claim 17, wherein the first and second requests are formed by a client.

20. (original): A method as described in claim 17, further comprising at least one of decoding the decrypted content and outputting the decoded content.

21. (original): A method as described in claim 17, wherein:

the persistent license was encrypted using an asymmetric encryption algorithm; and

the content, the boundary license, and the content license were encrypted using

respective symmetric encryption algorithms.

22. (original): One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 17.

23. (original): A client comprising:

a processor; and

memory configured to maintain:

a persistent license including a key that is encrypted; and

a playback application that is executable on the processor to:

form a request to access encrypted content, wherein the request:

is for communication to a licensing server; and

includes the persistent license;

receive a response to the request that includes the key; and

access the encrypted content utilizing the key.

24. (original): A client as described in claim 23, wherein the key is for decrypting the encrypted content.

25. (original): A client as described in claim 23, wherein:

the memory is further configured to maintain a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

26. (original): A client as described in claim 23, wherein:

the memory is further configured to maintain a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the content license using the key to obtain the content key; and

decrypt the content using the content key.

27. (original): A client as described in claim 23, wherein:

the memory is further configured to maintain a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

28. (original): A client as described in claim 23, wherein:

the memory is further configured to maintain a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the session license using the client key to obtain the session key;

decrypt the boundary license using the session key to obtain the boundary key;

decrypt the content license using the boundary key to obtain the content key; and

decrypt the content using the content key.

29. (original): A client as described in claim 23, wherein the playback application is further executable to:

form an initial request for:

communication to the licensing server; and

storing encrypted content by the playback application;

receive the persistent license in response to the initial request; and

store the encrypted content and the persistent license.

30. (original): A client as described in claim 23, wherein the playback application is further executable to form a request to obtain the encrypted content from another client.

31. (original): A client as described in claim 23, further comprising a tuner configured to receive the encrypted content when streamed over a network.

32. (original): A client as described in claim 23, wherein the license includes a certificate for verifying the licensing server.

33. (original): A system comprising:

a network;

a client including:

a persistent license having a key that is encrypted; and

a playback application that is executable to:

form a request to access encrypted content, wherein the request includes the persistent license;

receive a response to the request that includes the key; and

access the encrypted content utilizing the key; and

a licensing server including a licensing module that is executable to:

receive the request including the persistent license;

decrypt the persistent license to obtain the key; and

form the response that includes the key for communication to the client over the network.

34. (original): A system as described in claim 33, wherein:

the client includes a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

35. (original): A system as described in claim 33, wherein:

the client includes a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the content license utilizing the key to obtain the content key; and

decrypt the content utilizing the content key.

36. (original): A system as described in claim 33, wherein:

the client includes a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

37. (original): A system as described in claim 33, wherein:

the client includes a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the session license utilizing the client key to obtain the boundary key;

decrypt the boundary license utilizing the session key to obtain the boundary key;

decrypt the content license utilizing the boundary key to obtain the content key;

decrypt the content utilizing the content key; and

play the decrypted content.

38. (original): A system as described in claim 33, wherein the key is for decrypting the encrypted content.

39. (original): A system as described in claim 33, wherein the persistent license is encrypted with an asymmetric encryption algorithm and the server includes a server private key for decrypting the persistent license.

40. (original): A system as described in claim 33, wherein the playback application

is further executable to:

form an initial request for:

communication to the licensing server; and

storing encrypted content by the playback application;

receive the persistent license in response to the initial request; and

store the encrypted content and the persistent license.

41. (original): A system as described in claim 33, wherein the playback application is further executable to form a request to obtain the encrypted content from another client.

42. (original): A system as described in claim 33, wherein the encrypted content is streamed to the client over the network.

APPENDIX: EVIDENCE

None.

APPENDIX: RELATED PROCEEDINGS

None.